HELLENIC DATA
PROTECTION AUTHORITY

Athens, 16-10-2018

Ref.: C/ΕΞ/8187/16-10-2018

DECISION 65/2018

The Hellenic Data Protection Authority met in plenary session at its headquarters on Tuesday 9-10-2018, at the invitation of its President, to address the issue of maintaining or amending the draft list of the types of processing operations which are subject to the requirement for a data protection impact assessment following the opinion 7/2018 adopted by the European Data Protection Board (EDPB). The President of the Authority Konstantinos Menoudakos and the members Konstantinos Christodoulou, Antonios Symvonis, Spyridon Vlachopoulos, Konstantinos Lamprinoudakis (rapporteur), Haralambos Anthopoulos and Eleni Martsoukou (also rapporteur) were present. At the meeting, without the right to vote, were also present Efrosini Siougle, auditor, as assistant rapporteur, and Irini Papageorgopoulou, Department of Administrative Affairs, as secretary.

The Authority took note of the following:

By decision no. 53/2018 the Authority decided to draw up a draft list of the types of processing operations which are subject to the requirement for a data protection impact assessment (DPIA) pursuant to Article 35 (4) of the General Data Protection Regulation (EU) 679/2016 (GDPR). Before issuing such a list, the Authority, in accordance with Article 35 (6) of the GDPR, applied the consistency mechanism, referred to in Article 63, by announcing the draft list to the EDPB. The EDPB in its plenary session of 25 September 2018 adopted Opinion 7/2018[1] on the draft DPIA list of the Authority based on Article 64 (1) of the GDPR. In its opinion, for which the

[1]Opinion 7/2018 of the EDPB is available at: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-greece-sas-dpia-list_en

Authority was informed by electronic means on 2 October 2018, the EDPB requests the Authority to amend the draft list on the basis of the recommendations contained therein.

The Authority, having heard the rapporteurs and the assistant rapporteur and after a thorough debate,

REASONED IN ACCORDANCE WITH THE LAW

1. In accordance with Article 35 (1) of the GDPR:
   "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."
2. In accordance with Article 35 (3) of the GDPR, the DPIA is required in particular in the following cases:
   '(...) (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
   (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
   (c) a systematic monitoring of a publicly accessible area on a large scale (...)".
3. In order to provide a consistent interpretation of the processing operations requiring a DPIA in view of the high risk they are likely to represent, the Article 29 Working Party has adopted the *"Guidelines on Data Protection Impact Assessment (DPIA) and determining whether the processing "is likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248[2]), endorsed by the EDPB at its first plenary session. These guidelines primarily aim to clarify the concept of high risk

[2] The guidelines WP248 are available at https://edpb.europa.eu/node/70 and http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

and set the criteria for the establishment of the lists to be adopted by the Data Protection Authorities on the basis of Article 35 (4) of the GDPR. The text also aims at facilitating the work of the EDPB and the facilitation of controllers who are under an obligation to carry out an impact assessment.

4. In accordance with Article 35 (4) and (6) of the GDPR:

   "(paragraph 4) The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.";

   "(paragraph 6) Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union"

5. In accordance with Article 64 (1), (3), (6), (7) and (8) of the GDPR:

   "(paragraph 1) The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:
   (a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4); (...)".

   "(paragraph 3) In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. (...)".

   "(paragraph 6) The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3".

   "(paragraph 7) The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format".

   "(paragraph. 8) Where the supervisory authority concerned informs the Chair of

the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply".

6. In line with the recommendations set out in Opinion 7/2018, the EDPB requests the Authority to amend the draft DPIA list as follows:
    a. On the reference to the guidelines WP248: add that the draft list is based on the Guidelines WP248 "Guidelines for the Impact Assessment", which it complements and further specifies.
    b. On the concept of large-scale: delete the quantitative criteria and add a reference to the definitions of large scale as set out in the Guidelines for the Data Protection Officer (WP243) and the Impact Assessment (WP248).
    c. Concerning data processing carried out with the use of an implant: specify that only processing of health data with the use of an implant is subject to the requirement of an impact assessment.
7. In view of the above, the Authority, having taken into account and examined the above recommendations, unanimously considers that the opinion 7/2018 of the EDPB should be accepted, the necessary changes to the draft list initially submitted to the EDPB be made and the modified list be communicated to the EDPB.
8. To this purpose a) a reference is added that the DPIA list is based on the guidelines WP248, which it complements and further specifies, (b) the quantitative criteria that were included in the original draft DPIA list for the definition of the large scale processing are deleted and a reference to the relevant definitions in the guidelines WP243 and WP248 is added, and (c) point 2.2.5 of the DPIA ist is renumbered by removing the provision for the use of implants, as the processing of health data using implants is covered by point 2.1 and in conjunction with point 3.1.

FOR THESE REASONS

The Authority, acting unanimously, decides to amend the draft list of the types of processing operations which are subject to the requirement for a data protection impact assessment based on the recommendations of the EDPB Opinion 7/2018 and to communicate the modified list to the EDPB. The amended list is therefore as follows:

List of the kind of processing operations which are subject to the requirement for a data protection impact assessment according to article 35 par. 4 of GDPR

Legal basis

According to article 35 par. 4 of GDPR, the supervisory authority establishes and makes public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment (DPIA) pursuant to par. 1 and communicates this list to the European Data Protection Board (EDPB).

Where this list involves processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union, the consistency mechanism referred to in article 63 shall be applied.

Background

A DPIA is required when a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons (article 35 par. 1 of GDPR). Conducting a DPIA is required in particular in the cases referred to in article 35 par. 3 of GDPR.

In order to provide a more concrete set of processing operations for which a DPIA is required due to their inherent high risk, the Article 29 Working Party has adopted the guidelines entitled "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (WP248 rev.01). The above guidelines set out nine criteria that data controllers should use to determine whether or not a DPIA has to be carried out.

Definition of large scale

When determining whether the processing is carried out on a large scale, it is recommended that the following factors, in particular, be considered on the basis of the DPIA guidelines (WP248) as well as the guidelines entitled "Guidelines on Data Protection Officers ('DPOs')" (WP243):

a. the number of data subjects involved, either as a specific number or as a percentage of the relevant population;

b. the volume of data and / or the range of data items being processed;

c. the duration or the permanent nature of the data processing activity;

d. the geographical scope of the processing activity.

Kind of processing operations which are subject to DPIA

The present list groups and further specifies the kind of processing operations for which DPIA is required including indicative examples. This list is not exhaustive and does not remove or alter the obligation to conduct a DPIA in all cases where the conditions of article 35 par.1 of GDPR are met. This list is based on article 35 of GDPR and in particular par. 1 and 3 as well as the Working Party 29 guidelines on DPIA (WP248), which it complements and further specifies.

The criteria for carrying out a DPIA are grouped in the following three categories:

- *1st category:* based on the types and purposes of the processing.
- *2nd category:* based on the types of personal data and/or categories of data subjects.
- *3rd category:* based on the additional characteristics and/or means of the processing.

Conducting a DPIA shall be compulsory when at least one of the criteria of the 1st or the 2nd category is met. It shall also be compulsory when at least one of the criteria of the 3rd category is met and the processing concerns types and purposes of the 1st category, and/or types of personal data and/or categories of data subjects of the 2nd category.

1st category: types and purposes of the processing

1.1 Systematic evaluation, scoring, prediction, prognosis and profiling, especially of aspects concerning the data subject's economic situation, health, personal preferences or interests, reliability or behaviour, location or movements or the credit rating of data subjects.
Indicative examples include the case in which a financial institution screens its customers on the basis of credit reference data or anti-money laundering and counter-terrorist financing or fraud data, or the case in which a biotechnology company offers genetic tests directly to consumers in order to assess and predict the disease/health risks.

1.2 Systematic processing of personal data that aims at taking automated decisions producing legal effects concerning data subjects or similarly significantly affects data subjects and may lead to the exclusion or discrimination against individuals.
Indicative examples are the automatic refusal of an online credit application or e-recruiting practices without any human intervention (recital 71 of GDPR) or an automatic refusal of insurance provision.

1.3 Systematic processing of personal data which may prevent the data subject from exercising its rights or using a service or a contract, especially when data collected by third parties are taken into account.
Indicative examples are the case where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan or not, registering the data subject in a "black" list, such as the list of mobile operators or registering the data subject in whistleblowing systems.

1.4 Systematic processing of personal data concerning profiling for marketing purposes when the data are combined with data collected from third parties.

1.5 Large scale systematic processing for monitoring, observing or controlling natural persons using data collected through video surveillance systems or through networks or by any other means over a public area, publicly accessible area or private area accessible to an unlimited number of persons. It includes the monitoring of movements or location/geographical position on real time or not real time of identified or identifiable natural persons.
Indicative example are the use of video surveillance cameras in shopping malls/centers or public transportation stations, or the processing of location data of

passengers in the airport or in public transportation. Also, the wi-fi tracking of visitors in shopping centers or the processing of personal data using drones.

1.6 Large scale systematic processing of personal data concerning health and public health for public interest purposes as is the introduction and use of electronic prescription systems and the introduction and use of electronic health records or electronic health cards.

1.7 Large scale systematic processing of personal data with the purpose of introducing, organizing, providing and monitoring the use of electronic government services, as defined in article 3 of L.3979/2011 as applicable.

2nd category: types of personal data and/or categories of data subjects.

2.1 Large scale processing of special categories of personal data referred to in Article 9 par. 1 (including genetic data and biometric data for the purpose of uniquely identifying a natural person) and of personal data referred to in Article 10 of GDPR.

2.2 Large scale systematic processing of data of high significance or of a highly personal nature as are

2.2.1 Data of social welfare (data concerning poverty, unemployment, social work etc.),

2.2.2 Data of electronic communications, including the content of the communications such as electronic mail, metadata and data of geographic position/location, with the exception of telephone call recording pursuant to art.4 par.3 of L.3471/2006,

2.2.3 Data concerning the national identity number or other identifiers of general application or the alteration of the conditions and terms of processing and use of them and of other related to them personal data,

2.2.4 Data included in personal documents, diaries, notes from e-readers and in life-logging applications equipped with note-taking features and very personal information,

2.2.5 Data collected or generated by means of devices (such as these with sensors) especially through the 'internet of things – IoT' applications (such as smart televisions, smart household appliances, connected toys, smart cities, smart energy meters etc.) and/or by using other means.

2.1 Systematic monitoring – provided that it is fair – of the position/location of employees as well as of the content and of the metadata of employee communications with the exception of logging files for security reasons provided that the processing is limited to the absolutely necessary data and is specifically documented. A relative example that falls into the obligation of carrying out a DPIA is the use of DLP systems.

Processing of biometric data for the purpose of uniquely identifying a natural person as well as genetic data of employees.

3rd category: additional characteristics and/or means of the processing.

3.1 Innovative use or application of new technological or organizational solutions, which can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms, like the combined use of fingerprint and face recognition for improved physical access control, or mhealth applications, or other "smart" applications from which user profiles are generated (e.g. daily habits), or artificial intelligence applications as well as publicly accessible blockchains that include personal data.

3.2 Matching and/or combining personal data originating from multiple sources or third parties, or for two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subjects.

3.3 In case the processing concerns personal data that has not been obtained from the data subject and the information to be provided to data subjects pursuant to Article 14 of GDPR proves impossible or would require a disproportionate effort or is likely to render impossible or seriously impair the objectives of the processing.

Revision

The above list is subject to regular revisions every two years or to an unscheduled revision due to significant developments in technology or in operational models, as well as in the case of a change in the purposes of the processing when these new purposes present high risk.